REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are now in allowable form.

In addition, the Applicants' representative would like to thank Examiner Patel for kindly taking a substantial amount of time on February 9, 2005 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. REJECTION OF CLAIMS 1-13 AND 17 UNDER 35 U.S.C. § 102

Claims 1-13 and 17 stand rejected as being anticipated by the Pandya patent (United States Patent No. 6,671,724, issued December 30, 2003, hereinafter "Pandya"). In response, the Applicants have amended independent claim 1, from which claims 2-13 and 17 depend, in order to more clearly recite aspects of the invention.

Pandya teaches a system for managing network resources in a distributed networking environment. The system includes two main software components: a plurality of "agent" components deployed at various network devices, and one or more "control point" components deployed throughout the network. The agents monitor network resources, as well as the network devices with which they are associated, for example to assess the character and quantity of network resources that are required by the network devices. The agents report this information to the control points, which centrally coordinate and control the deployed agents and monitor the status of network resources. In response to monitored network conditions and the data reported by the agents, the control points may alter the behavior of particular agents in order to provide the required network services and resources to the networked devices.

The Examiner's attention is directed to the fact that Pandya fails to disclose or suggest the novel invention of a virtual private network in which master nodes control the admission and departure of subsets of member nodes, as claimed in Applicants'

independent claim 1 as amended. Specifically, Applicants' claim 1 positively recites:

1. A group management system comprising:
a plurality of interconnected nodes communicatively coupled with each other as member nodes of a virtual private network ("VPN"); and
a plurality of master nodes, each of the master nodes controlling admission and departure in the VPN for an associated non-empty subset of the member nodes. (Emphasis added)

The Applicants' invention is directed to methods and apparatuses for scalable distributed management of virtual private networks (VPNs). The management of encrypted group communications necessary to establish secure, private VPN communications channels through an underlying public network infrastructure places a variety of burdens on a VPN manager. In particular, the addition or removal of a member from a VPN often involves the generation and distribution of one or more new encryption keys that allow current VPN members to decrypt private communications sent through the VPN, but prevent non-VPN members from decrypting the communications. As VPN membership increases and changes dynamically with greater frequency, the complexity of encryption key management becomes even more burdensome. Thus, the VPN manager becomes a single point of failure for the entire VPN; overload of the VPN manager can cause the entire VPN to fail. This makes the VPN architecture very difficult and very costly to scale, which is not ideal for enterprises relying on secure and private electronic communications.

The Applicants' invention enhances the scalability of a VPN by dividing the member nodes of the VPN into subsets and providing a plurality of master nodes that are each associated with a subset of member nodes to control membership (*i.e.*, admission and departure) in the VPN for that subset. For example, each master node is responsible for managing the generation and distribution of encryption keys for only its associated subset(s), so that VPN communication and management burdens are not placed entirely on a single master node. This eliminates the single point of failure, because if one master node fails, any one of a plurality of other master nodes is available to assume the failed node's responsibilities. Moreover, a VPN employing such

an architecture is more easily scalable than a VPN employing a more conventional architecture, because a plurality of new member nodes may be added or admitted to the VPN through a discrete master node. The security and privacy afforded by traditional VPNs is still retained.

In contrast, Pandya teaches a distributed network comprising a plurality of interconnected computing devices, not a VPN. Specifically, Pandya does not teach or suggest a network architecture that provides secure, private communications channels between select network devices. The Examiner alleges that portions of Pandya (in particular column 9, lines 60-65) suggest that Pandya's system can be used as a VPN. However, the Applicants respectfully submit this portion of Pandya at most describes the advantages of Pandya's invention (*e.g.*, implementing policy-based quality of service between the application and transport layers of the network). That is, once good quality of service is established in the network, additional benefits such as the ability to use the network to operate a VPN are supported. This is not the same as using Pandya's network as a VPN.

Moreover, Pandya teaches a method for locally monitoring network devices in order to optimize network resource allocation among multiple devices, for example via local agents that report back to a central control point. In other words, Pandya controls and coordinates the activity of member nodes. Pandya does not address the need to control the admission and departure of nodes in the network in which the agents and the control points are deployed, for example through the management and distribution of encryption keys to select member nodes. Furthermore, nowhere does Pandya teach or even suggest the desirability of controlling the admission and departure of nodes from a group of nodes in the network, *e.g.*, in order to provide secure communications channels between networked devices. Pandya thus fails to teach or make obvious a system for scalably managing VPNs that controls the admission and departure of nodes from discrete VPN subsets, as positively claimed by the Applicants in amended claim 1. Therefore, for at least the reasons set forth above, the Applicants submit that independent claim 1, as amended, fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

Dependent claims 2-13 and 17 depend from claim 1 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 2-13 and 17 are not anticipated by the teachings of Pandya. Therefore, the Applicants submit that dependent claims 2-13 and 17 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

II. REJECTION OF CLAIMS 14-16 UNDER 35 U.S.C. § 103

Claims 14-16 stand rejected as being unpatentable over Pandya. The Applicants respectfully traverse the rejection.

Pandya has been discussed above. As discussed, Pandya fails to disclose or suggest the novel invention of a virtual private network in which master nodes control the admission and departure of subsets of member nodes in the VPN, as claimed in Applicants' amended independent claim 1, from which claims 14-16 depend. Moreover, nowhere does Pandya teach or even suggest the desirability of controlling or restricting the admission and departure of nodes in the network in which the agents and the control points are deployed, *e.g.*, in order to provide secure communications channels between networked devices. Pandya thus fails to teach or make obvious a system for scalably managing VPNs that controls the admission and departure of nodes from discrete VPN subsets, as positively claimed by the Applicants in claim 1. Therefore, for at least the reasons set forth above, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claims 14-16 depend from claim 1 and recite additional features therefore. As such, and for at least the reasons set forth above, the Applicants submit that claims 14-16 are not made obvious by the teachings of Pandya. Therefore, the Applicants submit that dependent claims 14-16 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants

believe that all of the presented claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

2/28/05
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Moser, Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702